FUJITSU Software
ServerView Infrastructure Manager V2.0

Operating Procedures

CA92344-1474-02
March 2017

Preface

Purpose

This manual provides overviews of the initial settings and the operating procedures or using FUJITSU Software ServerView Infrastructure Manager (hereafter referred to as ISM). ISM is software for simpler and more efficient operation and management of a multitude of ICT devices that are running in datacenters and server rooms.

Related Manuals

Manual Name	Notation in this Manual	Description
FUJITSU Software ServerView Infrastructure Manager V2.0 User's Manual	ServerView Infrastructure Manager V2.0 User's Manual	This manual describes the ISM functions, the installation procedure, and methods for operation and troubleshooting. It allows you to quickly grasp all functions and all operations of ISM.
FUJITSU Software ServerView Infrastructure Manager V2.0 Start Guide	ServerView Infrastructure Manager V2.0 Start Guide	This manual describes an overview of the functions and a workflow for installing ISM. It allows you to quickly grasp the procedures for installing ISM.
FUJITSU Software ServerView Infrastructure Manager V2.0 Operating Procedures	ServerView Infrastructure Manager V2.0 Operating Procedures	This manual describes the operating procedures for the initial setup and daily operation (monitoring of nodes, server setups, installation of OSes on servers, updating of server firmware) of ISM.
FUJITSU Software ServerView Infrastructure Manager V2.0 Glossary	ServerView Infrastructure Manager V2.0 Glossary	The glossary provides definitions of the terminology that you need to understand for using ISM.

Together with the manuals mentioned above, you can also see the latest information about ISM by accessing your local support.

For the respective hardware products for management, see the manuals of the relevant hardware.

For PRIMERGY, see "ServerView Suite ServerBooks" or the manual pages for PRIMERGY.

http://manuals.ts.fujitsu.com

Intended Readers

This manual is intended for readers who consider using the product for comprehensive management and operation of such ICT equipment and possess basic knowledge about hardware, operating systems, and software.

Notation in this Manual

Notation

Keyboard

Keystrokes that represent nonprintable characters are displayed as key icons such as [Enter] or [F1]. For example, [Enter] means press key labeled "Enter"; [Ctrl]+[B] means hold down the key labeled "Ctrl" or "Control" and then press the B key.

Symbols

Items that require your special caution are preceded by the following symbols

Point

Describes the content of an important subject.

Note

Describes an item that requires your attention.

Variables: <xxx>

Represents variables that require replacement by numerical values or text strings in accordance with the environment you are using.

Example: <IP address>

Abbreviation

You may see the following abbreviations in this manual.

Official name	Abbreviation	
Microsoft(R) Windows Server(R) 2016 Datacenter	Windows Server 2016 Datacenter	Windows Server 2016
Microsoft(R) Windows Server(R) 2016 Standard	Windows Server 2016 Standard	
Microsoft(R) Windows Server(R) 2016 Essentials	Windows Server 2016 Essentials	
Microsoft(R) Windows Server(R) 2012 R2 Datacenter	Windows Server 2012 R2 Datacenter	Windows Server 2012 R2
Microsoft(R) Windows Server(R) 2012 R2 Standard	Windows Server 2012 R2 Standard	
Microsoft(R) Windows Server(R) 2012 R2 Essentials	Windows Server 2012 R2 Essentials	
Microsoft(R) Windows Server(R) 2012 Datacenter	Windows Server 2012 Datacenter	Windows Server 2012
Microsoft(R) Windows Server(R) 2012 Standard	Windows Server 2012 Standard	
Microsoft(R) Windows Server(R) 2012 Essentials	Windows Server 2012 Essentials	
Microsoft(R) Windows Server(R) 2008 R2 Datacenter	Windows Server 2008 R2 Datacenter	Windows Server 2008 R2
Microsoft(R) Windows Server(R) 2008 R2 Enterprise	Windows Server 2008 R2 Enterprise	
Microsoft(R) Windows Server(R) 2008 R2 Standard	Windows Server 2008 R2 Standard	
Red Hat Enterprise Linux 7.3 (for Intel64)	RHEL 7.3	Red Hat Enterprise Linux or Linux
Red Hat Enterprise Linux 7.2 (for Intel64)	RHEL 7.2	
Red Hat Enterprise Linux 7.1 (for Intel64)	RHEL 7.1	
Red Hat Enterprise Linux 6.8 (for Intel64)	RHEL 6.8(Intel64)	
Red Hat Enterprise Linux 6.8 (for x86)	RHEL 6.8(x86)	
Red Hat Enterprise Linux 6.7 (for Intel64)	RHEL 6.7(Intel64)	
Red Hat Enterprise Linux 6.7 (for x86)	RHEL 6.7(x86)	
Red Hat Enterprise Linux 6.6 (for Intel64)	RHEL 6.6(Intel64)	
Red Hat Enterprise Linux 6.6 (for x86)	RHEL 6.6(x86)	

Official name	Abbreviation	
SUSE Linux Enterprise Server 12 SP1 (for AMD64 & Intel 64)	SUSE 12 SP1(Intel64) or SLES 12 SP1(Intel64)	SUSE Linux Enterprise Server or Linux
SUSE Linux Enterprise Server 12 (for AMD64 & Intel 64)	SUSE 12(Intel64) or SLES 12(Intel64)	
SUSE Linux Enterprise Server 11 SP4 (for AMD64 & Intel 64)	SUSE 11 SP4(Intel64) or SLES 11 SP4(Intel64)	
SUSE Linux Enterprise Server 11 SP4 (for x86)	SUSE 11 SP4(x86) or SLES 11 SP4(x86)	
VMware(R) vSphere(TM) ESXi 6.5	VMware ESXi 6.5	VMware ESXi
VMware(R) vSphere(TM) ESXi 6.0	VMware ESXi 6.0	
VMware(R) vSphere(TM) ESXi 5.5	VMware ESXi 5.5	

Terms

For the major terms and abbreviations used in this manual, see "ServerView Infrastructure Manager V2.0 Glossary."

High Risk Activity

The Customer acknowledges and agrees that the Product is designed, developed and manufactured as contemplated for general use, including without limitation, general office use, personal use, household use, and ordinary industrial use, but is not designed, developed and manufactured as contemplated for use accompanying fatal risks or dangers that, unless extremely high safety is secured, could lead directly to death, personal injury, severe physical damage or other loss (hereinafter "High Safety Required Use"), including without limitation, nuclear reaction control in nuclear facility, aircraft flight control, air traffic control, mass transport control, medical life support system, missile launch control in weapon system. The Customer, shall not use the Product without securing the sufficient safety required for the High Safety Required Use. In addition, Fujitsu (or other affiliate's name) shall not be liable against the Customer and/or any third party for any claims or damages arising in connection with the High Safety Required Use of the Product.

To Use This Product Safely

This document contains important information required for using this product safely and correctly. Read this manual carefully before using the product. In addition, to use the product safely, the customer needs to understand the related products (hardware and software) before using the product. Be sure to use the product by following the notes on the related products. Be sure to keep this manual in a safe and convenient location for quick reference during use of the product.

Modifications

The customer may not modify this software or perform reverse engineering involving decompiling or disassembly.

Disclaimers

Fujitsu Limited assumes no responsibility for any claims for losses, damages or other liabilities arising from the use of this product. The contents of this document are subject to change without notice.

Trademarks

Microsoft, Windows, Windows Vista, Windows Server, Hyper-V, Active Directory, and the titles or names of other Microsoft products are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.

Linux is a trademark or registered trademark of Linus Torvalds in the United States and other countries.

Red Hat and all trademarks and logos based on Red Hat are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.

SUSE and the SUSE logo are trademarks or registered trademarks of SUSE LLC in the United States and other countries.

Copyright

Contents

Chapter 1 Shared Operations

1.1 Display the Help screen

A help screen has been prepared to provide detailed descriptions for each screen in ISM2.0. Refer to the help screen for descriptions for the content displayed.

Select [?Help] - [Help for this screen] in upper right hand side of each screen while it is displayed.

1.2 Refresh the screen

Except for some screens, ISM acquires information when screens are displayed. The information in each screen will not be automatically updated while the screen is displayed. When you want to display the most recent information, execute the screen refresh procedure to refresh the screen.

If you select the refresh button (⟳Refresh), the information will be acquired again and the screen will be refreshed.

Chapter 2 Pre-configurations

ISM manages 4 in layers: datacenter, floor, rack, and node. The meaning of each is as follows.

- Datacenter

  Datacenter corresponds to the building layer. This layer supposes a datacenter model with multiple floors.

- Floor

  This layer supposes a floor space where multiple racks are placed.

  The floor view can be displayed on the dashboard.

  Also, 3D view displays 3D graphics of the floor units.

- Rack

  This layer supposes a server rack with multiple management target devices (nodes) mounted.

- Node

  Management Target Devices

Registration within each layer is done using the following procedure.

1. Registration of datacenters
2. Floor registration (Registration of which data center that the floor is situated in)
3. Rack registration (Registration of which floor the rack is situated in)
4. Arranging the rack on the floor (Registration of the rack's installation position on the floor)
5. Node registration (Registration of a node in a rack)

2.1 Register a datacenter

Register the "Datacenter" layer showing the facility housing the datacenter.

1. From the Global Navigation menu, select [Management] - [Datacenters] to display the [Datacenter List] screen.
2. Select the ➕ button to display the [Register Datacenter/ Floor/ Rack] wizard.
3. In [Object of Registration], select [Datacenter].
4. Enter the setting items, and then select the [Register] button. See the help screen for descriptions on the setting items.

   Help screen: [Management] - ["Datacenters" screen] - [Datacenter List] - [Register Datacenter/Floor/Rack]

This finishes the datacenter registration. After datacenter registration is finished, the corresponding datacenter will be displayed on the [Datacenter List] screen.

2.2 Register a floor

Register the [Floor] layer that signifies the machine room in the datacenter facility.

1. On the [Datacenter List] screen, select the ➕ button to display the [Register Datacenter/ Floor/ Rack] wizard.
2. In [Object of Registration], select [Floor].
3. Enter the setting items, and then select the [Register] button. For the [Datacenter] settings item, specify the datacenter registered in "2.1 Register a datacenter." See the help screen regarding other setting items.

   Help screen: [Management] - ["Datacenters" screen] - [Datacenter List] - [Register Datacenter/Floor/Rack]

This finishes the floor registration. After floor registration is finished, the corresponding floor is displayed on the [Datacenter List] screen.

2.3 Register a rack

Register the "Rack" layer that signifies the server racks on the floor.

1. On the [Datacenter List] screen, select the ✚ button to display the [Register Datacenter/ Floor/ Rack] wizard.
2. In [Object of Registration], select [Rack].
3. Enter the setting items, and then select the [Register] button. For setting items [Datacenter] and [Floor], select the datacenter and floor registered in "2.1 Register a datacenter" and "2.2 Register a floor" respectively. See the help screen regarding other setting items.

   Help screen: [Management] - ["Datacenters" screen] - [Datacenter List] - [Register Datacenter/Floor/Rack]

This finishes the rack registration. After rack registration is finished, the rack will be displayed on the [Datacenter List] screen.

2.4 Deploy a rack on the floor

Deploying a rack on the floor.

1. On the [Datacenter List] screen, select the floor where the rack should be deployed to display the [Details of Floor] screen.
2. From the [Actions] button, select [Set Rack Position] to display the [Set Rack Position] wizard.
3. Select the [Add] button to display the [Add Unlocated Rack] wizard.
4. Select the rack to be added and select the [Add] button.

   Set the position of the rack and select the [Apply] button. See the help screen for information on how to set the rack position.

   Help Screen: [Management] - ["Datacenter" screen] - ["Details of Floor" screen] - [Set Rack Position]

This finishes the rack deployment. After rack deployment is finished, the rack will be displayed on the [Details of Floor] screen.

2.5 Register a node

Node registration can be done either by detecting and registering existing nodes in the network, or by directly entering the node information. Only the method of detecting and registering nodes in the network can be executed on a server.

If the information registered in ISM and the information registered in the node does not match, the functionality of the ISM might be limited.

2.5.1 Detect nodes in the network and register nodes

1. From the Global Navigation menu, select [Registration] to display the [Node Registration] screen.
2. From the [Actions] button, select [Manual Discovery] to display the [Manual Discovery] wizard.
3. Enter the setting items and select the [Execute] button.

Setting items	Setting contents
IP address detection range	Set the search range by specifying the IP address range.
Account	Select from the following items. - iRMC/BMC: Select when you want to detect the server. - SNMP: Select when you want to detect the PRIMEQUEST or the water-cooled Rack CDU. - SSH + SNMP: Select when you want to detect the ETERNUS or the network switch.

Set the required item for each account.

Table 2.1 When selecting iRMC/BMC in [Account]

Setting items	Details
User Name	iRMC/BMC User Name
Password	iRMC/BMC Password
Port Number	iRMC/BMC Port Number (Default: 623)

Table 2.2 When selecting SNMP in [Account]

Setting items	Details
Version	Select SNMP Version
Port Number	SNMP Port Number (Default: 161)
Community	SNMP Community Name

Table 2.3 When selecting SSH in [Account]

Setting items	Details
User Name	SSH User Name
Password	SSH Password
Port Number	SSH Port Number (Default: 22)

4. When a node is detected, it will be output on the [Discovered Node List] screen.

   If the automatic refresh setting is disabled, the detection status is not refreshed.
   Specify the refresh period in the automatic refresh settings or select the refresh button to refresh the screen.

5. When the status is shown as [Complete], select the [Discovered Node List] tab.

6. Select the checkbox of the node to be registered.

7. On the [Discovered Node List] screen, select [Registration discovered nodes] to display the [Node Registration] wizard.

8. Follow the instructions in the [Node Registration] wizard and input the setting items. See the help screen for descriptions on the setting items.

Setting items	Setting contents
Node Name	Enter the node name. The following one-byte characters cannot be used. /\:*?"<>| xxxx_yyyy is already entered as node name by default. The character strings displayed in xxxx, yyyy are as follows. - xxxx The following character strings are displayed according to node type. In case of server, server-blade, mmb: SV In case of switch: SW In case of storage: ST In case of facility: CDU - yyyy They are serial numbers for the node. If the serial numbers are not collected manually, IP addresses are displayed.
Chassis Name	Enter the chassis name when PRIMERGY CX or PRIMEQUEST is discovered.

Setting items	Setting contents
	If nodes mounted on the same chassis are discovered, enter the chassis name of the node mounted on smallest number of the slots. In a case of the other nodes on the same chassis, the chassis names are automatically entered. The following one-byte characters cannot be used. /\:*?"<>| SV_zzzz is entered in the chassis name by default. The serial numbers of the chassis are displayed in zzzz. If the serial numbers are not collected in manual discovery, IP addresses are displayed.
Web i/f URL	Enter the URL when you access Web i/f on the node.
Details	Enter the details.

See the Help screen for the details of the discovered node list items.

Help screen: [Registration] - ["Registration" screen] - ["Discovered Node List" screen] - [Help]

9. After entering the registration information of the discovered node has been finished, select [Registration].

   This finishes the node registration.

   After node registration is finished, the corresponding node will be displayed on the [Node List] screen.

   If an OS is installed on the target node, implement the following procedures.

10. On the [Node List] screen, select the target node to select the [Details of Node] screen - [OS] tab.

11. Select [OS action] - [Edit OS Information].

    The settings on the Edit OS Information screen are as follows.

Setting items	Setting contents
OS Type	Select OS type.
OS version	Select the OS version.
OS IP address	After setting the IP version, enter the IP address of the OS management port (IPv4/IPv6 are supported).
Domain Name	Enter domain name in FQDN format.
Account	Enter the administrator account.
Password	Enter the password of the administrator account.
OS Connection Port Number	Enter the port number for connecting to the OS. If using Windows it is the port number of the WinRM service (default setting is 5986), if using Linux it is the port number of the SSH service (default setting is 22). If not entered, the default port number will be set.

12. After entering the OS information, select [Apply].

This finishes OS information editing. After OS information editing is finished, the OS information on the corresponding node can be acquired.

2.5.2 Register a node directly

1. From the Global Navigation menu, select [Registration] to display the [Node Registration] screen.

2. From the [Actions] button, select [Registration] and the [Node Manual Registration] wizard is displayed.

3. Follow the instructions in the [Node Manual Registration] wizard and input the setting items. See the help screen for descriptions on the setting items.

   Help screen: [Registration] - ["Registration" screen](d)[Discovered Node List] - [Registration(node)]

4. Below is the description for the [Account] setting items in [1.Node Information] in the [Node Manual Registration] wizard.

Table 2.4 If server was selected in [Node Type]

Setting items		Details
iRMC		When not accessing the node through iRMC, uncheck the checkbox (Default: Checked).
	User Name	iRMC User Name
	Password	Password of iRMC User
	Port Number	iRMC Port Number (Default: 623)

Table 2.5 If "switch" or "storage" was selected in [Node Type]

Setting items		Details
SSH		When not accessing the node through SSH, uncheck the checkbox (Default: Checked).
	User Name	User name of the switch or storage
	Password	User Password of the switch or storage
	Port Number	SSH Port Number (Default: 22)
SNMP		When not accessing the node through SNMP, uncheck the checkbox (Default: Checked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the switch or storage

Table 2.6 If "facility" was selected in [Node Type]

Setting items		Details
SNMP		When not accessing the node through SNMP, uncheck the checkbox (Default: Checked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the switch or storage

Table 2.7 If "other" was selected in [Node Type]

Setting items		Details
iRMC/BMC		When accessing the node through iRMC/BMC, check the checkbox (Default: Unchecked).
	User Name	User Name of iRMC/BMC
	Password	User Password of iRMC/BMC
	Port Number	iRMC/BMC Port Number (Default: 623)
SSH		When accessing the node through SSH, check the checkbox (Default: Unchecked).
	User Name	Node User Name
	Password	Password of Node User
	Port Number	SSH Port Number (Default: 22)
SNMP		When accessing the node through SNMP, check the checkbox (Default: Unchecked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the node

From the Global Navigation menu, select [Management] - [Nodes] to display the [Node List] screen.

It may take time to display the node list depending on the number of nodes registered in ISM.

This finishes the node registration.

After node registration is finished, the corresponding node will be displayed on the [Node List] screen.

If an OS is installed on the target node, implement the following procedures.

5. On the [Node List] screen, select the target node to select the [Details of Node] screen - [OS] tab.
6. Select [OS action] - [Edit OS Information].

   The settings on the Edit OS Information screen are as follows.

Setting items	Setting contents
OS Type	Select OS type.
OS version	Select the OS version.
OS IP address	After setting the IP version, enter the IP address of the OS management port (IPv4/IPv6 are supported).
Domain Name	Enter domain name in FQDN format.
Account	Enter the administrator account.
Password	Enter the password of the administrator account.
OS Connection Port Number	Enter the port number for connecting to the OS. If using Windows it is the port number of the WinRM service (default setting is 5986), if using Linux it is the port number of the SSH service (default setting is 22). If not entered, the default port number will be set.

7. After entering the OS account information has been finished, select apply.

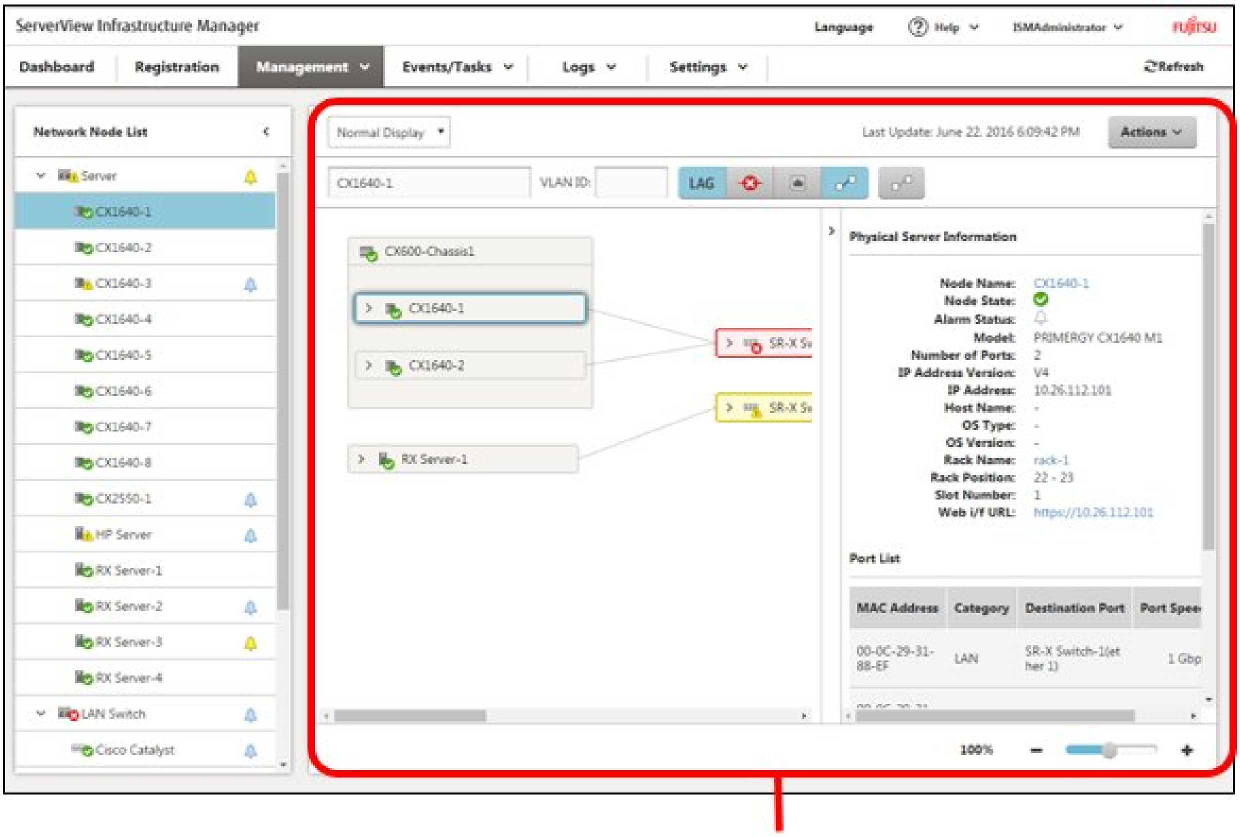
This finishes the node registration. After node registration is finished, the corresponding node will be displayed on the [Node List] screen.

2.6 Set up network connection

The Network Map displays the physical connections of LAN cables among the managed nodes. In the case of LLDP (Link Layer Discovery Protocol) of the network port on the managed node is enabled, ISM retrieves the connection relation among the nodes and displays the connections on the Network Map. However, if the managed node does not support LLDP or is not enabled, the connections are not displayed automatically. In that case, you can manually set up connections between respective nodes.

1. From the Global Navigation menu, select [Management] - [Network Map] to display the [Network Map Display] screen.

2. From the [Actions] button, select [Refresh Network Information] and select [Yes] to execute.



Last Update: June 22, 2016 6:09:42 PM

CX1640-1 VLAN ID:

Physical Server Information

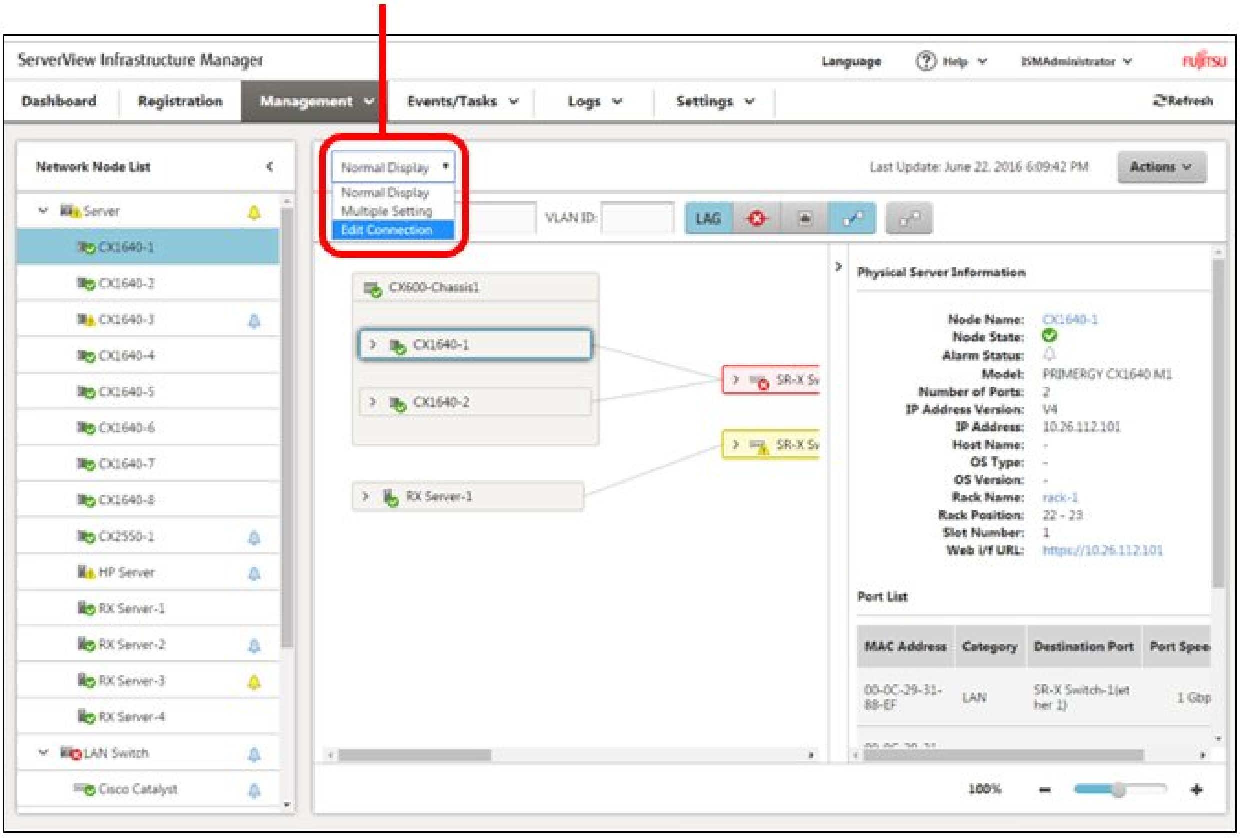
Node Name: CX1640-1
Node State: ✓
Alarm Status:
Model: PRIMERGY CX1640 M1
Number of Ports: 2
IP Address Version: V4
IP Address: 10.26.112.101
Host Name: -
OS Type: -
OS Version: -
Rack Name: rack-1
Rack Position: 22 - 23
Slot Number: 1
Web i/f URL: https://10.26.112.101

Port List

MAC Address	Category	Destination Port	Port Spee
00-0C-29-31-88-EF	LAN	SR-X Switch-1(ether 1)	1 Gbp

[Network Map Display] Screen

3. Select [Edit Connection] from the [Display Mode] pull-down menu.



[Display Mode] Pull-down menu

Last Update: June 22, 2016 6:09:42 PM

Physical Server Information

Node Name: CX1640-1
Node State:
Alarm Status:
Model: PRIMERGY CX1640 M1
Number of Ports: 2
IP Address Version: V4
IP Address: 10.26.112.101
Host Name: -
OS Type: -
OS Version: -
Rack Name: rack-1
Rack Position: 22 - 23
Slot Number: 1
Web I/F URL: https://10.26.112.101

Port List

MAC Address	Category	Destination Port	Port Spee
00-0C-29-31-88-EF	LAN	SR-X Switch-1(ether 1)	1 Gbp

4. Select the ❯ mark within the icon of the node to be connected to display the network port (▀).

5. Select the 2 ports to be connected. Select the [Add] button and the additional connections are displayed in gray.

6. Repeat the procedure 3 to 5 as many times as the number of the connections you wish to add.

7. On the [Network Map Display] screen, select [Edit Connections Saved] from the [Actions] button.

8. On the [Edit Connections Saved] screen, confirm the contents of the connections set up, then select the [Save] button.

9. In [Display Mode], select [Normal Display].

This finishes the procedure of network connection set up.

2.7 Set an alarm

Set up of the external notifications for ISM, based on the alarm detected when a node failure occurred, (such as the various traps received from a node, or events detected by monitoring function of ISM).

The followings are the notification methods.

- Execute a script
- Send an e-mail
- Transfer the received trap to an external SNMP manager

When sending e-mails, it is possible to encrypt the message with S/MIME.

When making the alarm settings, it should be done in the order of Action settings (notification method) - Alarm settings.

1. Preparations are required before Action settings (notification method).

   According to Action settings type (notification method), do the following settings respectively.

   [If executing scripts]

   a. Prepare script file.
   b. FTP is used to send it to ISM-VA. Access the ftp://<ISM-VA IP Address>/<User Group Name>/ftp/actionscript over FTP and store script files there.
   c. Log in to the ISM-VA console as the administrator user.
   d. Execute the ismadm event import - type script command.

      When executing the command, the script files stored in the FTP by each user will be imported in a batch.

   [If sending e-mails]

   a. On the [Alarms] screen, select [SMTP Server] to display the [SMTP Server settings] screen.
   b. From the [Actions] button, select [Edit] to display the [SMTP Server Settings] wizard.
   c. Enter the setting items, select the [Apply] button. (For help on entering the setting items, move to [Settings] - ["Alarms" screen] - ["SMTP Server" screen] - [Edit "SMTP Server"], and refer to Help on [Edit "SMTP Server"].)

      When sending an encrypted e-mail, do the following settings as well.
   d. Prepare personal certificate.

      Check that the certificate is in PEM format and that the certification and recipient mail address is encrypted.
   e. FTP is used to send it to ISM-VA. Access the ftp://<ISM-VA IP Address>/<User Group Name>/ftp/cert using FTP and store the certificate there.
   f. Log in to the ISM-VA console as the administrator user.
   g. Execute the ismadm event import - type cert command.

      When executing the command, the certificates stored in the FTP by each user will be imported in a batch.

   [If transferring traps]

   a. On the [Alarms] screen, select [SNMP Manager] to display the [SNMP Manager Settings] screen.
   b. From the [Actions] button, select [Add] to display the [Add SNMP Manager] screen.
   c. Enter the setting items, select the [Apply] button. (For help on entering the setting items, move to [Settings] - ["Alarms" screen] - ["SNMP Manager" screen] - [Add "SNMP Manager"], and refer to Help on [Add "SNMP Manager"].)
2. From the Global Navigation menu, select [Settings] - [Alarms] to display the [Alarm Settings] screen.
3. Select [Actions] to display the [Actions List] screen.
4. From the [Actions] button, select [Add] to display the [Add Action] wizard.
5. Enter the setting items and select the [Apply] button. (For help on entering the setting items, move to [Settings] - ["Alarms" screen] - [Add (Alarm)], and refer to Help on [Add (Alarm)].)
6. After action addition is finished, the corresponding action will be displayed on the [Actions List] screen.
7. On the [Alarms] screen, select [Common Alarm Settings] to display the [Common Alarm Settings] screen.
8. From the [Actions] button, select [Edit] to display the [Edit Common Alarm Settings] wizard.
9. Enter the setting items and select the [Apply] button. (Foe help on entering the setting items, move to [Settings] - ["Alarms" screen] - ["Common Alarm Settings" screen], and refer to Help on [Common Alarm Settings].)
10. On the [Alarms] screen, select [Alarms] to display the [Alarm List] screen.
11. From the [Actions] button, select [Add] to display the [Add Alarm] wizard.
12. Follow the [Add Alarm] wizard and enter the setting items. (For help on entering the setting items, move to [Settings] - ["Alarms" screen] - [Add (Alarm)], and refer to Help on [Add (Alarm)].)

13. After alarm addition is finished, the alarm will be displayed on the [Alarm List] screen.

This finishes the setup of node failure notifications.

2.8 Make settings for receiving SNMP traps

2.8.1 Change in SNMP settings

Set up a community name (SNMPv1/v2c). The default community name is set as "public" and this can be changed as required.

1. Log in to the ISM-VA console as the administrator user.
2. Execute the command ismadm snmp set - name <new community name>.

2.8.2 Add MIB file

You need to get an MIB file(s) individually to import it in ISM if you monitor the hardware, such as HP's servers, CISCO's switches, etc., supplied by vendors other than FUJITSU LIMITED.

1. Prepare an MIB file(s). Note that if the MIB file has any dependency relationship, all the target files are required.
2. FTP is used to send it to ISM-VA. Access ftp://<IP address of ISM-VA>/Administrator/ftp/mibs via FTP, and store all the MIB file(s).
3. Log in to the ISM-VA console as the administrator user.
4. Execute the command ismadm mib import. Executing the command causes all the MIB file(s) stored in FTP to be imported in batch.

2.9 Set a log collection schedule

ISM follows the schedule set (example: every day at 23:00) and collects and accumulates node logs on a regular basis. It is possible to have different settings for each node. The set schedule can be executed and log collection done at any time.

1. From the Global Navigation menu, select [Management] - [Nodes] to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

2. Select the node to be configured from the node list.
3. Select the [Log Settings] tab.
4. Execute [Edit Log Collection Settings] from the [Log Setting Action] button in the [Log Settings] tab.
5. Do the required settings on the settings screen, then select [Apply].

   - After selecting [Schedule Type], select the [Add] button and set the log collection time.
   - Check the [Enable Schedule execution] box. If the check is disabled, the created schedule will not be executed.
   - When the node is a server, [Operating System Log] and [ServerView Suite Log] can be selected as targets for log collection if the OS information is set correctly.

     However, [Hardware Log], [ServerView Suite Log] cannot be selected depending on the server type. In this case, log cannot be collected.

6. Using the operations above, the log of the specified node will automatically be collected at the set time and accumulated in ISM.
7. When the log collection occurs according to the arbitrary timing in the settings, selecting the [Log Setting Action] button in the [Log Settings] tab and selecting [Collect Logs] executes the log collection. The [Collect Logs] operation will be registered as an ISM task. From the Global Navigation menu, select [Events/Tasks] - [Tasks] to confirm that the task has been completed.

2.10 Delete a node

Delete a registered node.

1. From the Global Navigation menu, select [Management] to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

2. Select the node to be deleted.
3. From the [Actions] button, select [Delete Node].
4. Confirm that the node to be deleted is correct, and then select [Delete].
5. After node deletion is finished, the corresponding node will be deleted from the [Node List] screen.

This finishes node deletion.

2.11 Delete a rack

Delete a registered rack.

1. From the Global Navigation menu, select [Datacenters] to display the [Datacenter List] screen.
2. Select the rack to be deleted.
3. From the [Actions] button, select [Delete Rack].

   See the help screen regarding things to be careful about when deleting a rack.

   Help Screen: [Management] - ["Datacenters" screen] - ["Details of Rack" screen] - [Delete Rack]

4. Confirm that the rack to be deleted is correct, and then select [Delete].

2.12 Delete a floor

Delete a registered floor.

1. On [Datacenter List] screen, select the floor to be deleted.
2. From the [Actions] button, select [Delete Floor].
3. See the help screen regarding things to be careful about when deleting a floor.

   Help Screen: [Management] - ["Datacenters" screen] - ["Details of Floor" screen] - [Delete Floor]

4. Confirm that the floor to be deleted is correct, and then select [Delete].

2.13 Delete a datacenter

Delete a registered datacenter.

1. On [Datacenter List] screen, select the datacenter to be deleted.
2. From the [Actions] button, select [Delete Datacenter].

   See the help screen regarding things to be careful about when deleting a datacenter.

   Help Screen: [Management] - ["Datacenters" screen] - ["Details of Datacenter" screen] - [Delete Datacenter]

3. Confirm that the datacenter to be deleted is correct, and then select [Delete].

Chapter 3 Node Monitoring

3.1 Operate the dashboard

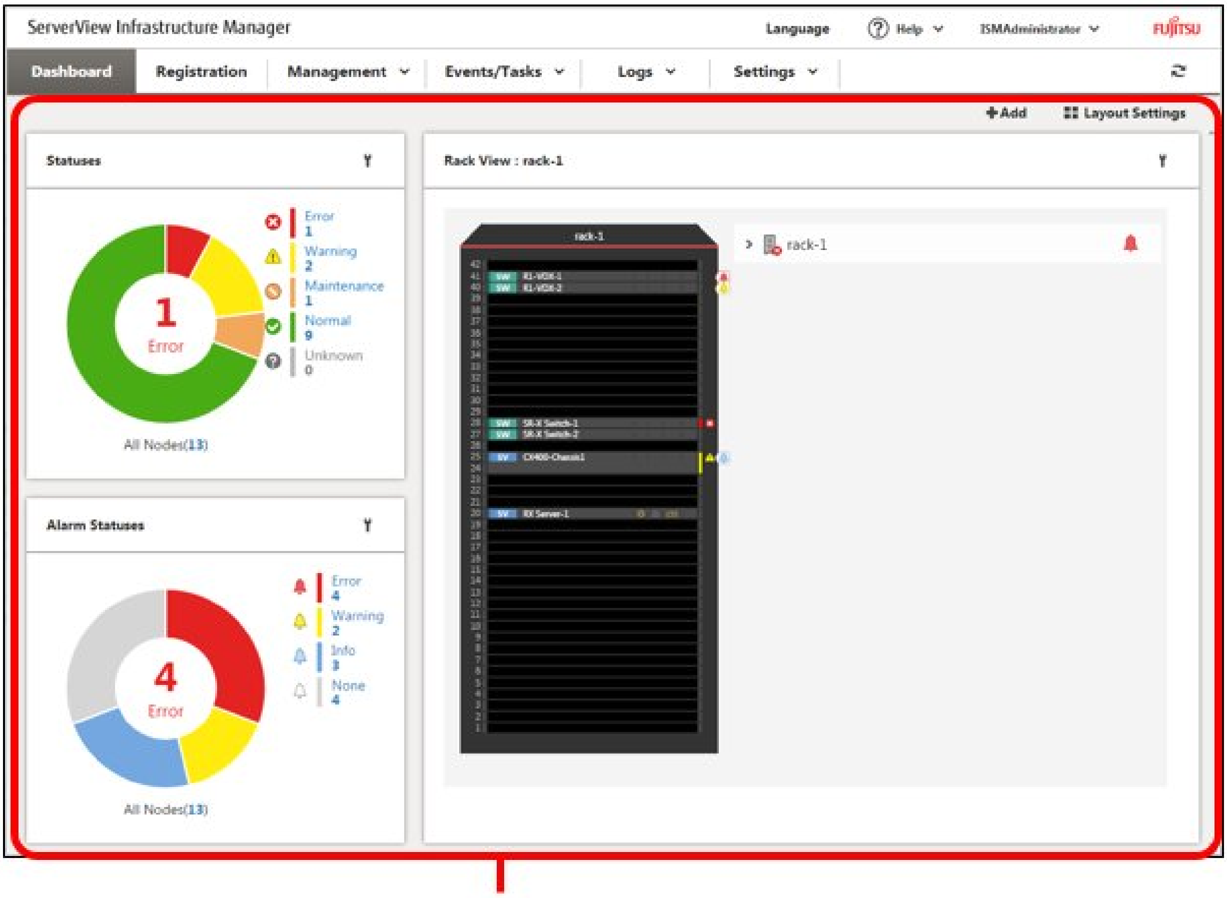
The dashboard displays the widget showing various information about status, logs etc. Select the widget according to the needs of the user. The information required can be referenced.

See the help screen [Dashboard] - [Dashboard Customization] for help on how to select the widget to be shown on the dashboard.

3.2 Check the status of a node

The node status can be checked in the [Statuses] widget on the dashboard or on the [Node List] screen.

1. Check the node status using the [Statuses] widget on the dashboard.



[Dashboard] screen

2. See the help screen for details regarding the [Statuses] widget.

   Help screen: Select [Dashboard] - [Dashboard Widget] - [Statuses], and see [Statuses] for help.

3. In the [Statuses] widget, select the status to check (Error, Warning, Maintenance, Normal, and Unknown) to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

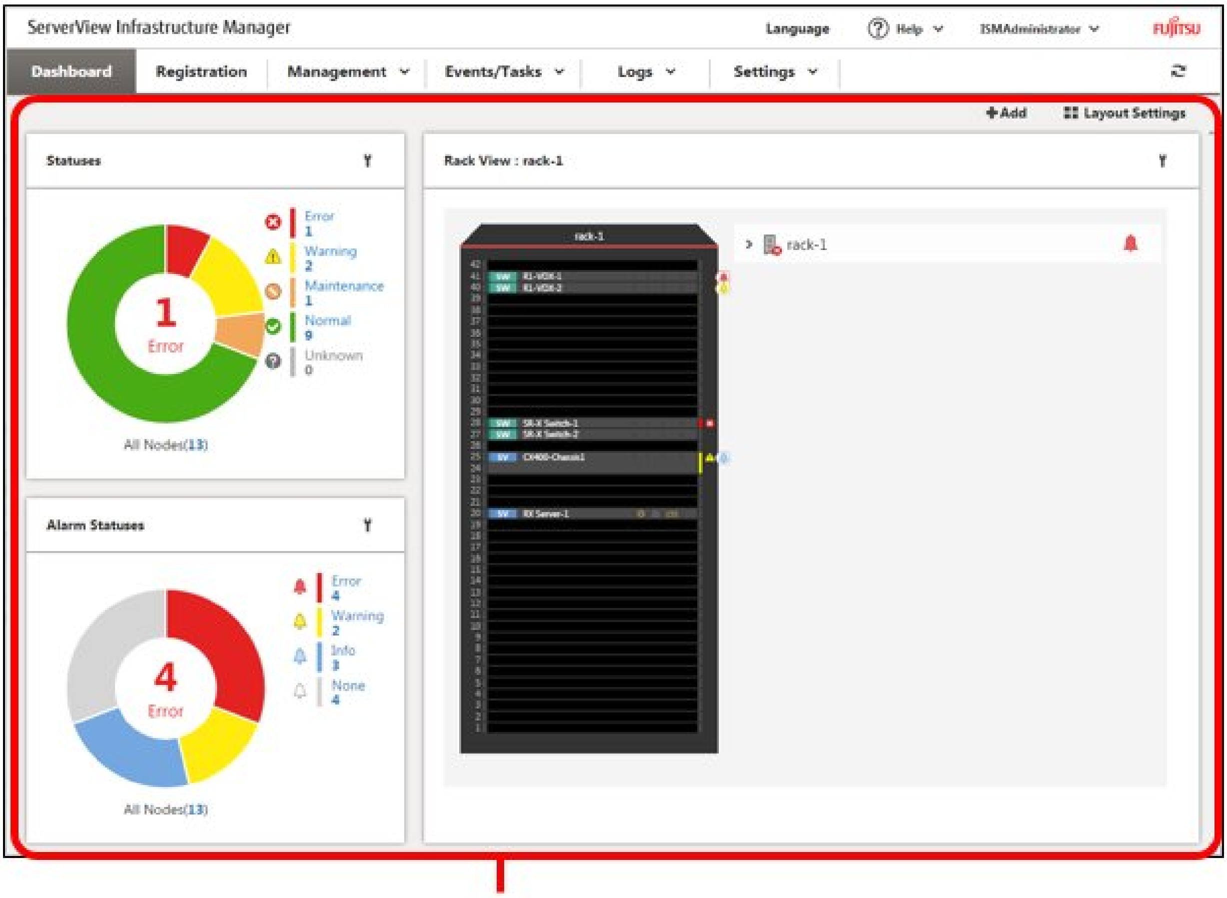
4. The status of the node is displayed. (For help regarding the contents displayed, move to [Management] - ["Nodes" screen], and see the ["Nodes" screen] for Help.)

This finishes the node status display.

3.3 Display the node notification information

The node status, as well as whether an event has occurred on the node can be checked using either the [Alarm Statuses] widget on the dashboard or by checking the [Node List] screen.

1. From the Global Navigation menu, select [Dashboard] to display the [Dashboard] screen.



[Dashboard] screen

2. For help on descriptions on the [Alarm Statuses] widget, move to [Dashboard] - [Dashboard Widget] - [Alarm Statuses] and see [Alarm Statuses] for help.

3. In the [Alarm Statuses] widget, select the status to be checked (Error, Warning, Info, and None) to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

4. The nodes with the alarm status will be displayed. (For help regarding the contents displayed, move to [Management] - ["Nodes" screen], and see the ["Nodes" screen] for Help.)

This finishes the display of the node notification information.

3.4 Display the node log

Displaying the logs collected from the managed node lined up in a time series. By specifying the requirements of the managed node, Severity, Category (Hardware, operating system) etc., the logs to be displayed can be narrowed down.

1. From the Global Navigation Menu, select [Logs] - [Node Logs] to display the [Node Log Message List] screen.

2. When narrowing down the node logs displayed, select the [Filter] button to display the [Filter] wizard. Enter the filtering requirements into the [Filter] wizard, and then select the [Filter] button. (For help on filtering conditions, move to [Logs] - ["Node Logs" screen] - [Filter (Node Logs)], and see Help on [Filter (Node Logs)]).

3. The filtered node logs will be displayed on the [Node Log Message List] screen.

This finishes the node logs display.

3.5 Download the Archived Logs

The archived logs collected from the managed node can be downloaded.

1. From the Global Navigation Menu, select [Logs] - [Archived Logs] to display the [List of Archived Logs] screen.
2. Check the checkbox of the node whose archived logs should be downloaded.
3. From the [Actions] button, select [Create Download Files] to open the [Create Download Files of Archived Logs] wizard.
4. Enter the setting items and select the [Run] button. (For help on setting items, move to [Logs] - ["Archived Logs" screen] - [Create Download Files (Archived Logs)] - ("Archived Logs" screen)], and refer to Help on [Create Download Files of Archived Logs ("Archived Logs" screen)].
5. The download file is created.
6. From the [Actions] button, select [Check Download Files] to show the [List of Archived Logs] wizard.
7. When selecting the [Download] button, the download file created in step 5 will be downloaded to the console.

This finishes the download of the archived logs.

Chapter 4 Operations for each use scene

4.1 Check the node where a failure occurred

Since among all the nodes, only the managed nodes where a failure is currently occurring are displayed, it is easy to check the information of failed nodes.

ISM does not update the status of the nodes on the screen in real time. In order to display the current status of the node, select the refresh button to refresh the screen.

1. From the Global Navigation menu, select [Dashboard].
2. In the [Statuses] widget, select the [Error] on the right side of ❌.
3. Only the nodes where an error has occurred will be displayed.
4. Check the status for the abnormal nodes displayed.

4.2 Display the node logs of the target node

Information collection about a node error checks if there is an error in the contents of the node log that has been collected and displayed.

1. To display the log correctly, the already collected logs will be processed before collecting the most recent log.

   From the Global Navigation Menu, select [Logs] - [Node Logs] to display the [Node Log Message List] screen. If the node logs have been shown previously, the messages will be displayed in the list. Delete logs as required.

   [Delete Logs]

   a. On the [Node Log Message List] screen, select the [Actions] button - [Delete Log] to open the [Delete Logs] wizard.

   b. Enter the setting items, then press the [Delete] button. (For help on setting items, move to [Logs] - ["Node Logs" screen] - [Delete Logs], and refer to Help on [Delete Logs].)

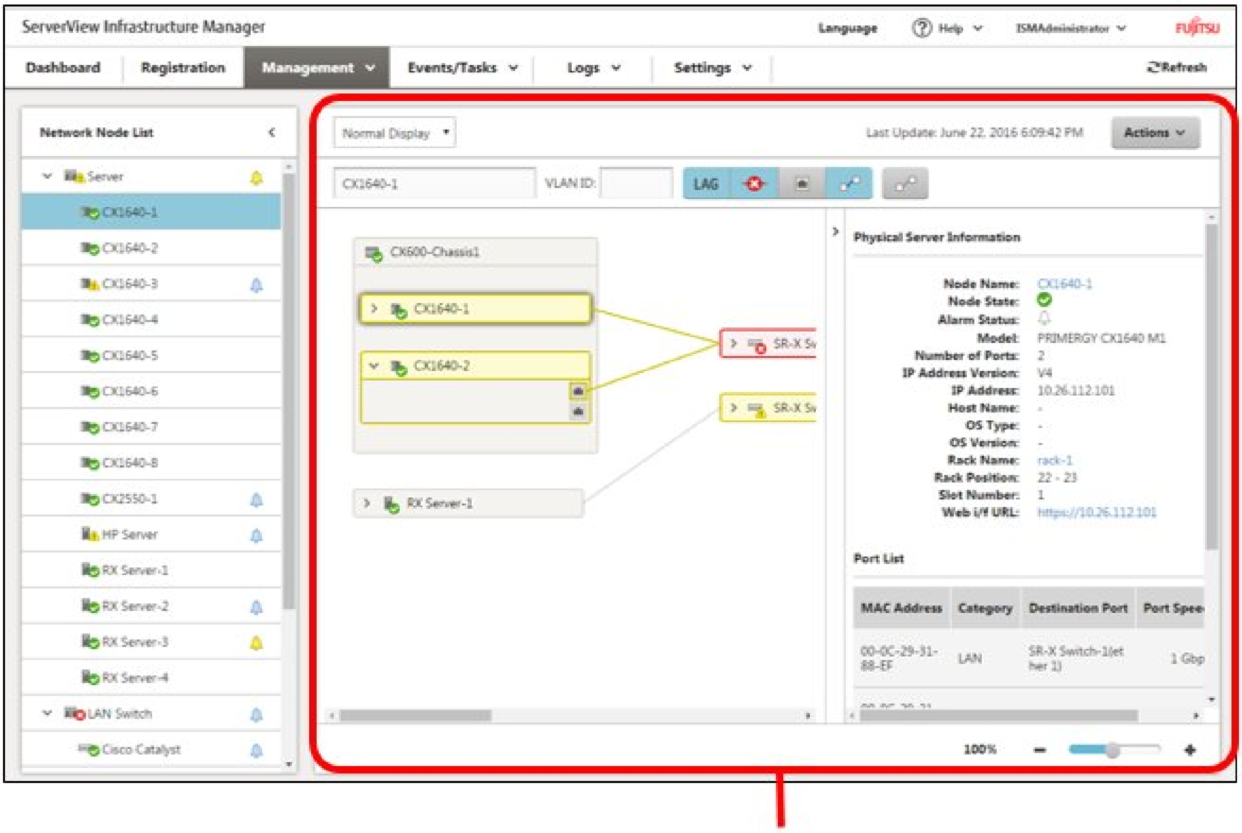
2. Select [Actions] - [Collect Logs] to display the [Collect Logs] wizard.
3. Press the [Select] button, and then select nodes on the [Select applicable node(s)] screen displayed.
4. By selecting the [Run] button on the [Collect Logs] screen, collection is executed.
5. Since collection happens in the background, the results are not reflected immediately. When the update button in selected, depending on the collection status, any collected messages will be added.

This finishes the node log display.

4.3 Check the failed network point and its affected area

You can graphically check the failed network point and its affected area with the Network Map.

1. From the Global Navigation menu, select [Management] - [Network Map] to display the [Network Map Display] screen.



Last Update: June 22, 2016 6:09:42 PM

Physical Server Information

Node Name: CX1640-1
Node State: ✓
Alarm Status: 🔔
Model: PRIMERGY CX1640 M1
Number of Ports: 2
IP Address Version: V4
IP Address: 10.26.112.101
Host Name: -
OS Type: -
OS Version: -
Rack Name: rack-1
Rack Position: 22 - 23
Slot Number: 1
Web I/F URL: https://10.26.112.101

Port List

MAC Address	Category	Destination Port	Port Spee
00-0C-29-31-88-EF	LAN	SR-X Switch-1(ether 1)	1 Gbp

[Network Map Display] Screen

2. Check the node indicated in red. The node where an error occurs turns red.

3. If the [Switching display affected area of error] button on the top of the Network Map is OFF, change it to ON.

4. The connection in the affected area, the port frame or the node frame is displayed in yellow.

   If virtual networks are configured, the virtual machines within the affected area, the virtual switches, and the virtual connections are also displayed in yellow.

This finishes the check for failed network point and its affected area.

4.4 Set up server

4.4.1 Set up server BIOS

Set up BIOS for server registered in ISM.

For the BIOS settings procedure, see "4.4.6 Assign profile."

4.4.2 Set up server iRMC

Set the iRMC of the servers registered in ISM.

For the iRMC settings procedure, see "4.4.6 Assign profile."

4.4.3 Install server OS

Install OSes on the servers registered in ISM.

The following OSes can be installed.

- Windows Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- VMware

1. Preparing environment configurations

   When installing an OS, it is required to create a DHCP server.

   For details, access your local support.

2. Preparing the OS image

   As a preparation setting when installing an OS, it is necessary to first import the OS image into the repository. For the repository management, see "2.3.2 Repository Management" in the "User's Manual."

3. Create a profile (or set up)

   OS installation is executed by the profile assignment. To install an OS, a profile must be created or set up.

4. Assigning a profile

   The OS registered in the profile, after the profile assignment, will be installed.

   For the procedure on profile assignment, see "4.4.6 Assign profile."

4.4.4 Create policy

The template containing information regarding node hardware settings or information on OS installation is called a policy. When a lot of nodes are managed, input into the profile is simplified by policies specified by common factors. Creating this policy. It is optional to create a policy and it is not always required when creating a profile.

1. From the Global Navigation menu, select [Settings] - [Profiles] to display the [Profile Settings] screen.
2. On the [Profile Settings] screen, select [Policies] tab to display the [All Policies] screen.
3. From the [All Policies] screen, select [Actions] button - [Add Policy] to display the [Add Policy] wizard.

   - If setting the BIOS policy

     On the [1.General Information] screen on the [Add Policy] wizard, select [BIOS] in the field of [Policy Type].

   - If setting iRMC policy

     On the [1.General Information] screen on the [Add Policy] wizard, select [iRMC] in the field of [Policy Type].

   Follow the [Add Policy] wizard and enter the other setting items. (For help on setting items, move to [Settings] - ["Profiles" screen (Settings)] - [Policy/Policy Group List] - [Add Policy], and refer to Help on [Add Policy].)

4. After policy addition is finished, the corresponding policy will be displayed on the [All Policies] screen.

This finishes policy creation.

4.4.5 Create profile

Profiles are collections of settings for node hardware or OS installation, they need to be created individually for each node.

1. Create a policy. For creating a policy, see "4.4.4 Create policy." A policy is not always required for creating a profile.

   Moreover, already created policies can be applied.

2. On the [Profile Settings] screen, select the [Profiles] tab - the [All Profiles] to display the [All Profiles] screen.
3. From the [All Profiles] screen - [Actions] button, select [Add Profile] to display the [Add Profile] wizard.
4. Follow the instructions on the [Add Profile] wizard and enter the setting items.

Point

For help on entering setting items, move to [Settings] - ["Profiles" screen] - [Profile/Profile Group List] - [Add Profile], and see Help on [Add Profile].

[If setting up BIOS using policy]

a. In the [Add Profile] wizard - [1.General Information] - [BIOS Policy], select the created policy (or a policy to be reused).

b. Enter the other setting items on the [1.General Information] screen and select [Next].

c. In the [2. Details] - [BIOS] tab, the setting values with the selected policies are automatically entered.

d. Set the required items as required.

[If setting up iRMC using policy]

a. In the [Add Profile] wizard - [1.General Information] - [iRMC Policy], select the created policy (or a policy to be reused).

b. Enter the other setting items on the [1.General Information] screen and select [Next].

c. In the [2. Details] - [iRMC] tab, the setting values with the selected policies are automatically entered.

d. Set the required items as required.

[If installing an OS]

a. In the [Add Profile] wizard - [1.General Information] - [OS Type], select the OS type to be installed.

b. Enter the other setting items on the [1.General Information] screen and select [Next].

c. Select the [2. Details] - [OS] tab to enter the setting items.

d. Select the [2. Details] - [OS Information] tab to enter the setting items.

5. After profile addition is finished, the corresponding profile will be displayed on the [All Profiles] screen.

This finishes profile creation.

4.4.6 Assign profile

Assign the profile to the servers registered in ISM, set up the server BIOS/iRMC and install an OS.

1. Create a profile. (For creating a profile, see "4.4.5 Create profile.")
2. From the Global Navigation menu, select [Management] - [Nodes] to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.
3. In [Column Display], select [Profile].
4. From the node list, select the nodes where the profile should be assigned.
5. From the [Actions] button, select [Assign/Reassign Profile] to show the [Profile Assignment] wizard.
6. Follow the instructions on the [Profile Assignment] wizard and enter the setting items. (For help on setting items, move to [Management] - ["Nodes" screen] - [Assign/Reassign Profile], and see Help on [Assign/Reassign Profile].)
7. After the BIOS/iRMC settings or the OS installation is finished, the [Status] field on the [Node List] screen will display [Assigned] for the corresponding server.

This finishes the node profile application.

4.5 Check firmware version of the server

Display the firmware version of the servers registered in ISM.

1. From the Global Navigation menu, select [Management] - [Nodes] to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

2. Select the name of the target server and select [Properties].

3. From the [Actions] button, select [Get Node Information] to start collecting node information.

4. From the Global Navigation menu, select [Management] - [Nodes] to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

5. In [Column Display], select [Firmware].

6. On the [Node List] screen, the firmware version of the server will be displayed in the [Current Version] column.

This finishes the check of the firmware version of the server.

4.6 Update the server firmware

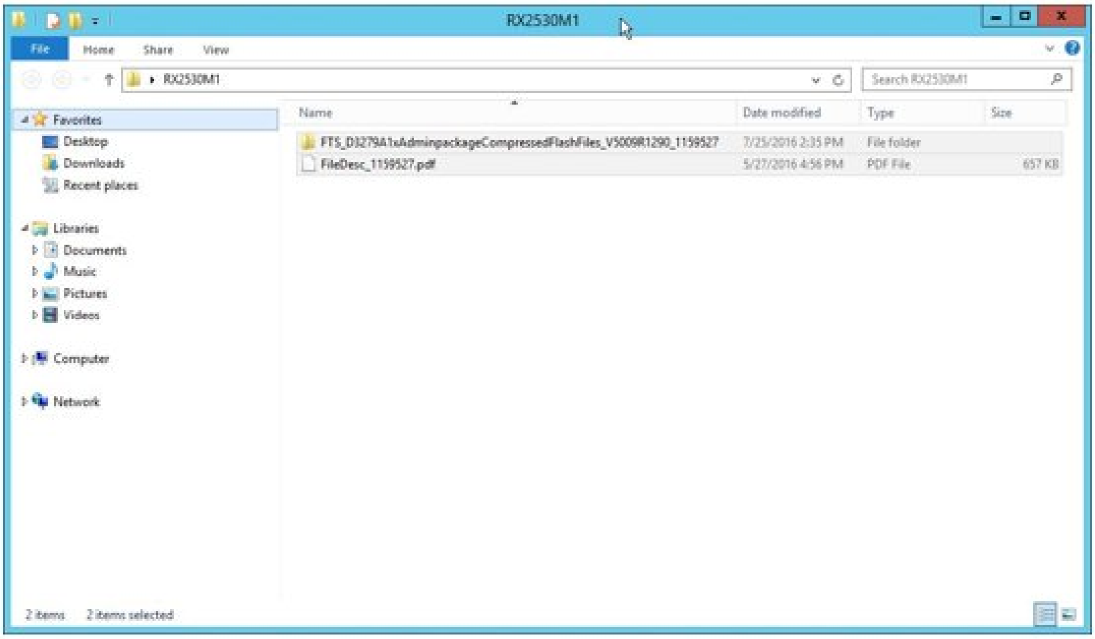
Updating the firmware of the servers registered in ISM.

1. If the firmware to be updated is not imported yet, the firmware must first be imported. If it is already imported, proceed to step 7.

2. Download the firmware of the iRMC/BIOS from the website. Download the firmware for the target model from the website below.

   http://support.ts.fujitsu.com/

3. Store the downloaded file in any folder. If the downloaded file is compressed, decompress the file in the folder.



Name	Date modified	Type	Size
FTS_D3279A1xAdminpackageCompressedFlashFiles_V5009R1290_1159527	7/25/2016 2:35 PM	File folder	
FileDesc_1159527.pdf	5/27/2016 4:56 PM	PDF File	657 KB

4. FTP is used to send it to ISM-VA. Make sure to transfer it with the same structure as the folder.

   Transfer them by using FTP command or FTP client software (such as FFFTP or WinSCP). At the time, set the character code as UTF-8 to be converted.

   Note

   Do not use Windows Explorer because the character code is not handled correctly.

   After logging in to ISM-VA with the FTP client software, move from the root directory to the "<user group name>/ftp" directory and transfer the data into this directory.

5. Import firmware.

   On the GUI screen of ISM -the Global Navigation Menu, select [Settings] - [Repositories]. From the [Actions] button in [Firmware], select [Import Firmware].

   Follow the instructions on the screen and enter the file location, type, model and version, then select the assignment.

   Enter versions to be entered using the table below.

Type	Model	Version Entering Method
iRMC	RX100 S8, CX2550 M1, etc.	Refer to the release notes and specify the versions of iRMC and SDR.
BIOS	RX100 S8, CX2550 M1, etc.	Refer to the release notes and specify the BIOS version.

   After starting the import, the operations will be registered as ISM tasks. Check the status of the operations on the "Tasks" screen.

   From the Global Navigation menu, select [Events/Tasks] - [Tasks] to display a list of the tasks in the [Tasks] screen.

6. Check that the firmware has been imported.

   From the Global Navigation menu, select [Settings] - [Repositories] to display the [Repository Settings] screen. Select [Firmware] on the left side of the screen, select the [Firmware] tab on the right side of the screen.

   Check that the imported firmware is displayed on the [Firmware List] screen.

7. Set the target server to maintenance mode.

   From the Global Navigation menu, select [Management] - [Nodes] to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

   Select the node that is target for firmware update, select [Actions] - [Maintenance Mode Settings] and put it in maintenance mode.

8. Select target server.

   In [Column Display], select [Firmware].

   Select the checkbox of the node where firmware update should be done.

   (If a firmware with a higher version number than the current one is imported, the checkbox cannot be selected unless the version number of this firmware is displayed in the latest version column).

   From the [Actions] button, select [Update Firmware] to display the [Update Firmware] wizard.

9. Starting firmware update.

   Follow the instructions on the [Update Firmware] wizard and enter the setting items. (For help on setting items, move to [Management] - ["Nodes" screen] - [Update Firmware], and see Help on [Update Firmware].)

   After starting the firmware update, the operations will be registered as ISM tasks.

   Check the status of the operations on the "Tasks" screen.

   From the Global Navigation menu, select [Events/Tasks] - [Tasks] to display a list of the tasks in the [Tasks] screen.

10. If you update the BIOS and PCI cards with online firmware update, restart the target server.

11. Cancel maintenance mode for the target server.

    From the Global Navigation menu, select [Management] - [Nodes] to display the [Node List] screen.

    Select the server target for firmware update, select [Actions] - [Maintenance Mode Settings] and cancel maintenance mode.

12. Check that the firmware version of the target server has been updated.

    From the Global Navigation menu, select [Management] - [Nodes] to display the [Node List] screen.

    Select the node name of the device where firmware update was done and select [Properties].

    From the [Actions] button, select [Get Node Information] to start collecting node information.

    From the Global Navigation menu, select [Management] - [Nodes] to display the [Node List] screen.

    On the [Node List] screen - [Column Display], select [Firmware] to display the version number after updating.

This finishes the server firmware update.

4.7 Set up switch and storage

4.7.1 Create profile

Create a profile (aggregate of hardware settings).

1. On the [Profile Settings] screen, select the [Profiles] tab - the [All Profiles] to display the [All Profiles] screen.
2. From the [All Profiles] screen - [Actions] button, select [Add Profile] to display the [Add Profile] wizard.
3. Follow the instructions on the [Add Profile] wizard and enter the setting items.

   Enter RAID configuration, SNMP settings, account and other settings for each device.

   (For help on setting items, move to [Settings] - ["Profiles" screen (Settings)] - [Profile/Profile Group List] - [Add Profile], and see Help on [Add Profile].)
4. After profile addition is finished, the corresponding profile will be displayed on the [All Profiles] screen.

This finishes profile creation.

4.7.2 Assign profile

Assign the profile to the node registered in ISM.

1. Create a profile. (For creating profile, see "4.7.1 Create profile.")
2. From the Global Navigation menu, select [Management] - [Nodes] to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.
3. In [Column Display], select [Profile].
4. From the node list, select the nodes where the profile should be assigned.
5. From the [Actions] button, select [Assign/Reassign Profile] to show the [Profile Assignment] wizard.
6. Follow the instructions on the [Profile Assignment] wizard and enter the setting items. (For help on setting items, move to [Management] - ["Nodes" screen] - [Assign/Reassign Profile], and see Help on [Assign/Reassign Profile].)
7. After assignment of the profile has been finished, on the [Node List] screen the [Status] column of the node will be displayed as [Assigned].

This finishes the node profile application.

4.7.3 Change in VLAN settings of LAN Switch

Changing VLAN settings of LAN switch from the Network Map.

1. From the Global Navigation menu, select [Management] - [Network Map] to display the [Network Map Display] screen.
2. From the pull-down menu on the top of the screen, select [Multiple Setting].
3. By LAN Switch on the Network Map, select the port to change the VLAN settings.
4. Select [Action] - [Multiple VLANs setting] to enter the setting changes.
5. Confirm the changes and select [Registration] to execute the setting changes if there is no problem.
6. Refresh the network management information after the execution, and then confirm that the changes are applied on the Network Map.

This finishes the VLAN setting changes.

4.7.4 Change in Link Aggregation of LAN switch

Changing Link Aggregation of LAN switch from the Network Map.

1. From the Global Navigation menu, select [Management] - [Network Map] to display the [Network Map Display] screen.
2. Select [Action] - [LAG Setting].
3. Select the node to change the Link Aggregation settings, then select either of [Add], [Change] or [Delete].
4. Enter the setting change, select [Confirmation].
5. Confirm the changes and select [Registration] to execute the setting changes if there is no problem.
6. Refresh the network management information after the execution, and then confirm that the changes are applied on the Network Map.

This finishes the Link Aggregation setting changes.

4.8 Power Capping

In ISM, specifying the upper limit of power consumption by each rack enables to curb the power consumption of mounted devices.

The upper limit of the power consumption is configured by each of the power capping policy (definitions according to the operational pattern).

The power capping policy operates two types of custom definitions, one definition for schedule operation, and one definition for the minimum power consumption operation (Minimum), by switching the four types in total.

In order to use power capping, it is required beforehand to set [Add power capping settings] (the node information for the power capping target and definition for power capping policy) to enable power capping policies.

Note

Power capping policy is managed by each rack. It is required to review the power capping settings (node power settings, the upper limit value for power capping policy) related to each rack.

- Add a node to the rack
- Remove a node from the rack
- Move a node to another rack

4.8.1 Confirm the current power capping status

Confirm the power capping status of the target rack.

1. In the [Datacenter List] screen, select the rack that you want to confirm the power capping setting status for.
2. Confirm the contents in the power capping setting status displayed in the upper right side of the rack details screen.

Power capping status	Details
Power capping not set up	Power capping has not been set up.
Power capping stopped	Power capping has been set up but all power capping policies are disabled. To enable it, select the [Actions] button to select [Enable/Disable Power Capping].
Power capping	Power capping has been set up and at least one power capping policy is enabled.
Power capping is updating	The power capping settings are being updated.
There is a discrepancy in the power capping	A node was added or deleted after the power capping was set up. It is required to enter the node power settings of the added device and to review the upper limit of the power capping policy.

4.8.2 Add/change the power capping settings of the rack

Register or edit the power capping definitions of the target rack.

1. In the [Datacenter List] screen, select the rack that you want to add or edit the power capping policy for.
2. Select the following from the [Action] button.
    - If adding a new power capping setting: [Add power capping setting]
    - If editing all the set power capping policy settings: [Edit power capping settings]

    The displayed content as well as the setting contents are displayed below.

    Rack power consumption column

    The current power capping status value is displayed.

Item	Details
Current status	Displays the latest status of the power capping settings.
The currently enabled policy	Displays the policy that has been enabled in [Enable/Disable Power Capping].
Maximum power consumption	Displays the total maximum power consumption value currently entered in the node power settings.
Fixed power value	Displays the entered total fixed power value (the total maximum power value of devices not using power capping).
Power consumption	The current total power consumption of the devices capable of power capping (mainly servers) and the maximum power consumption of devices that does not use power capping.

[Node power settings] tab

Enter the settings value of the nodes using power capping.

Item	Details
Node type	Type of each node.
Node Name	Name of each node.
Fixed power	Use the maximum power consumption value entered as a fixed value. Check if handling it as a fixed power. In a case of the device not collecting the power consumption value, this will be enabled automatically.
Maximum power consumption	Enter the maximum power consumption value as specification in catalogs. When doing internal calculations it is used as the possible range of node power capping. For devices where power capping cannot be used it is calculated using appropriate fixed power values.
Power consumption	Displays the current power consumption value retrieved from the nodes.
Business priority	- Low If the power reaches to the upper power value, it becomes the target for the power capping. - Middle If capping the power for Low devices is not enough, it will be the power capping target. - High If capping the power for Low and Middle devices are not enough, it will be the power capping target. - Critical Out of scope for power capping. However, if minimum policy is enabled power capping will be used.

[Power capping policy] tab

Register the setting values for the three types of power capping policies.

For the upper limit power consumption target, upper limit values for two types of custom policies, upper limit value for schedule policy as well as schedule can be set.

Item		Details
Power capping policy		
	Custom 1,2	Operation will be done with the set upper limit value specified for power consumption.
	Schedule	If schedule policy is enabled, operations will be done using the specified upper limit value during the duration of the schedule (day, time).
	Minimum	Operations will be done using minimal power consumption, including devices whose business priority is Critical.
Displayed value		
	Upper limit value	Enter the upper limit target value for each policy.
	Fixed value	The total value of the maximum power consumption of the devices that are out of scope for power capping.
	Enable/Disable	Displays the status of the power capping policy.
Detailed schedule settings		
	All day	Check if not specifying operating time.
	Set time	Check if setting start time and completion time. - Start time Set the time to start using scheduled power capping. Set the value in the ISM-VA time zone. - Completion time Set the time to complete operating scheduled power capping. Set the value in the ISM-VA time zone.
	Day	Check the day when scheduled power capping should be done. Multiple days can be selected.

Note

The upper limit value is the power capping target value. Whereas the capping is normally implemented to make sure that the power consumption is lower than the upper limit, if the upper limit is set low it may exceed the power consumption.

Point

If setting it as in the example below, it will be scheduled from Sunday 23:00 to Monday 5:00 in the ISM-VA time zone.

Setting Example)

- Start time: 23:00
- Completion time: 5:00
- Day: Sunday

4.8.3 Enable the power capping policy of the racks

Enable the power capping policy for the applicable racks.

1. In the [Datacenters List] screen, select the rack that you want to activate power capping policy for.
2. From the [Action] button, select [Enable/Disable power capping policy].
3. In the row of the power capping policy you want to activate, set [Enable/Disable] - [After Changing] to [Enable], then select [Apply].

   The displayed content is as follows.

Item	Details
Policy Name	Name of the power capping policy. There are four types: custom 1, custom 2, schedule, and minimum.
Upper limit value	The upper limit target value entered for each policy in the power capping settings.
Fixed value	The total value of the maximum power consumption of the devices that are out of scope for power capping.
Enable/Disable	Displays the status of the power capping policy.

Note

- Whereas all power capping policies are enabled independently, if minimum is set it is executed with highest priority. In this case, it will be operated with the minimum power consumption also for devices where the business priority in [Node power settings] in the power capping settings is Critical.
- If multiple power capping policies other than minimum are enabled, the policy with the lowest upper power consumption limit value will be executed.

4.8.4 Delete power capping settings for racks

Delete all power capping settings information for the rack.

1. In the [Datacenters List] screen, select the rack that you want to delete the power capping settings for.
2. From the [Action] button, select [Delete power capping settings].
3. Confirm that it is the rack that the settings should be deleted for, then select the [Delete] button.